HW4 Name: Sergio Coronado Date: 01/23/16

Goal: To use python to do a preliminary analysis of trraffic on a port by port basis

Approach: The python code was written by writing a class that would contain the parsed data. The data file to parse is passed through the program parameters followed by the name of a file to output the chart to. An example of the usage is as follows:

$ ./Coronado.HW.4.py < data_file> < plots utput_output_file >

The libraries used for this program where matplotlib . It was used for plotting the data. After, parsing the individual packets the data was then broken down into two separate data sets for incoming and outgoing packages. Lists for inter-arrival times, elapse times and counts per time interval were created each data set. For each data stream a list of pkt counts and byte counts was created in a per port basis. The data was repacked in such a way that system ports had counts calculated on a per port basis while reserved ports and user ports had counts calculated for every 100 and 100 ports respectively. Teh data was normalized and displayed in four different graphs.

Results:

The data showed that most of the traffic occurs in the system ports and user ports. The traffic on the user port area is scattered around different ports and the data had to be packed into bins to get a better show of the results. The figures below where created such that the system port counts where graphed per individual port while the user port and reserved ports where graphed per 50 and 100 ports respectively. Figure 1. shows that the amount of incoming packets is highly concentrated near the lower reserved port and the user ports with very little traffic on the system ports.

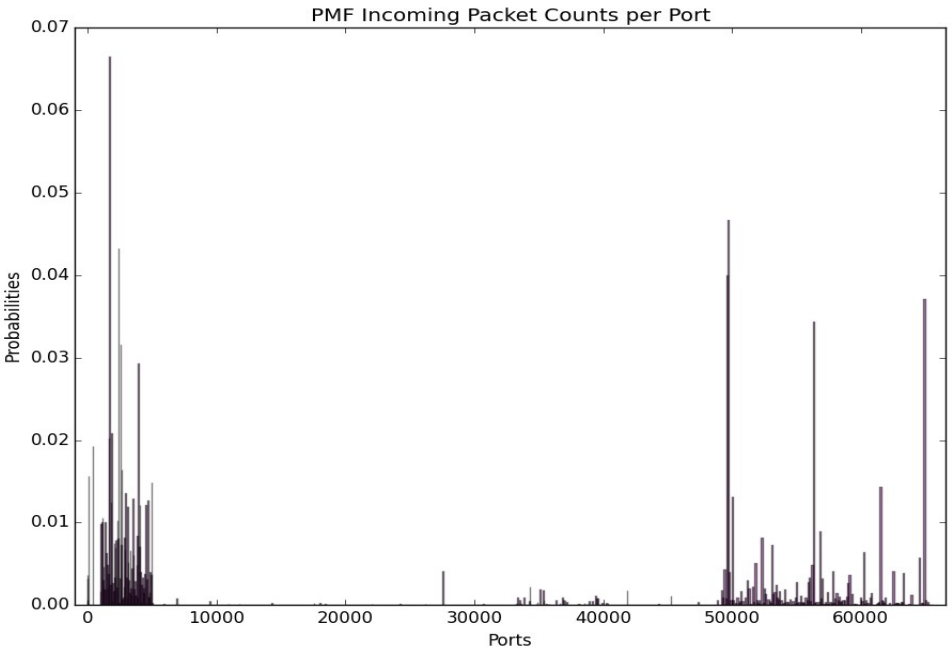

Figure 1. Incoming Packet counts per port.

In fact the statistics output by the program found that the port with the most packet counts was port

49730 the reason why the figure does not denote this is because the frequency of ports with higher packet counts is highest around the lower reserved ports with spikes occurring only in unique user ports. When looking at the outgoing trafffic it was observed that most of the packet traffic occurred in the user ports with exception of a large spike in port 80 the HTTP port.

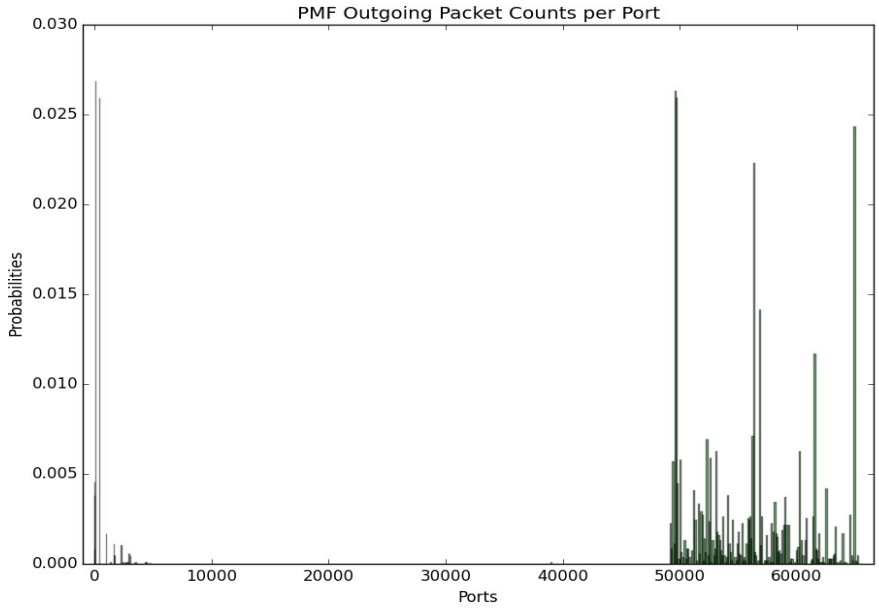

Figure 2. Outgoing Packet Counts per Port

When looking at the byte counts per port Figure 3 shows the incoming byte traffic reflects that of the incoming packet traffic, with most of the traffic concentrating between the lower reserved ports and the user ports and having the traffic in the lower reserved ports having a tighter concentration than on the user ports. Once again however the port with the most traffic was found to be 49730.

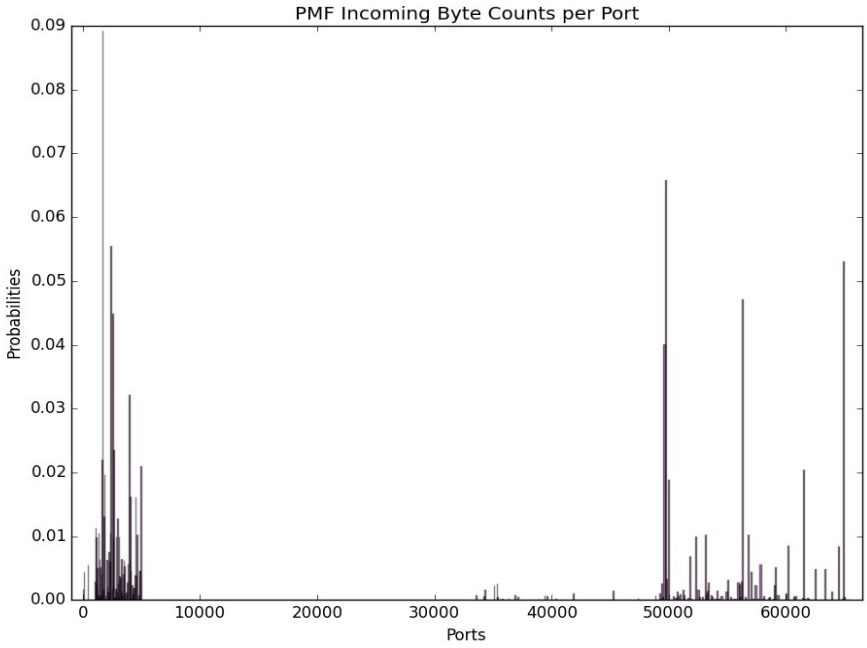

Figure3. Incoming Byte Counts per Port

The outgoing byte traffic differed from the outgoing packet count in the fact that most of the byte traffic seemed to be concentrated around the lower reserved ports and the port 80 this could be explained by the fact that there is probably a web-server somewhere in the topography, while most of the packet traffic is in the form of requests that can very likely be of 0 byte length the webserver on port 80 will likely respond with larger byte packets since it will be serving content.

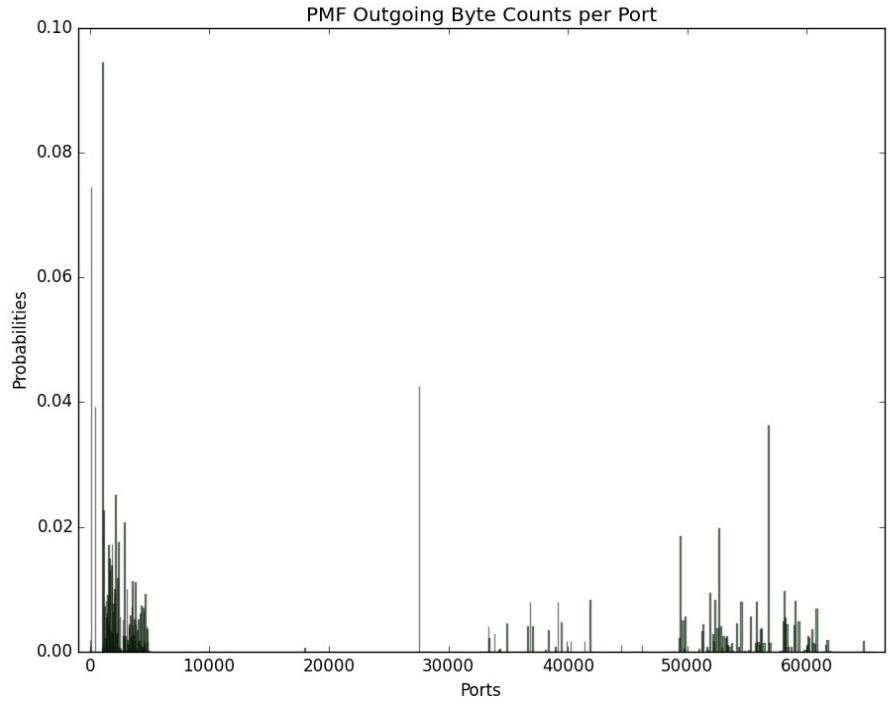

Figure 4. Outgoing Byte Counts per port

Statistical Results:

/////////////// Incoming Stats ///////////////
Total Bytes: 14541135
Max Bytes per Port:954232
Port with most byte traffic: 49730
Total Packets: 14455
Max Packets per Port: 659
Port with most packet traffic: 49730

/////////////// Outgoing Stats ///////////////
Total Bytes: 4084215
Max Bytes per Port:366460
Port with most byte traffic: 1029
Total Packets: 10682
Max Packets per Port: 287
Port with most packet traffic: 80